September 13, 1999
Preliminary Version

Congruence Subgroups and Rational Conformal Field Theory†

Antoine Coste

CNRS Laboratory of Theoretical Physics,
building 210, Paris XI University
91405 Orsay cedex, France

Antoine.Coste@th.u-psud.fr

Terry Gannon

Department of Mathematical Sciences,
University of Alberta
Edmonton, Canada, T6G 2G1

tgannon@math.ualberta.ca

Abstract

We address here the question of whether the characters of an RCFT are modular functions for some level N, i.e. whether the representation of the modular group $\mathrm{SL}_2(\mathbb{Z})$ coming from any RCFT is trivial on some congruence subgroup. We prove that if the matrix T, associated to $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, has *odd* order, then this must be so. When the order of T is even, we present a simple test which if satisfied — and we conjecture it always will be — implies that the characters for that RCFT will also be level N. We use this to explain three curious observations in RCFT made by various authors.

This is the presubmission copy. We are interested in receiving any feedback.

† The published version of this paper will assume slightly more mathematical sophistication; both versions have equivalent content but this one is a little more pedagogical.

1. Introduction

Associated to a rational conformal field theory (RCFT), or related structures such as affine Kac-Moody algebras or rational vertex operator algebras (VOAs), is a finite-dimensional representation ρ of the (homogeneous) modular group $\mathrm{SL}_2(\mathbb{Z})$. In particular, we write[1] $S := \rho\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T := \rho\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. S determines the fusion coefficients N_{ab}^c in the RCFT, by Verlinde's formula:

$$N_{ab}^c = \sum_{d\in\Phi} \frac{S_{ad}\, S_{bd}\, S_{cd}^*}{S_{0d}} \tag{1}$$

where $a, b, c, d \in \Phi$ label the finitely many primary fields. This modular representation is realised by the characters $\mathrm{ch}_a(\tau)$, $a \in \Phi$, of the RCFT:

$$\mathrm{ch}_a(-1/\tau) = \sum_{b\in\Phi} S_{ab}\, \mathrm{ch}_b(\tau) \tag{2a}$$

$$\mathrm{ch}_a(\tau+1) = \sum_{b\in\Phi} T_{ab}\, \mathrm{ch}_b(\tau) \tag{2b}$$

Basic known properties of ρ (i.e. S and T) will be quickly reviewed in §2.

In this paper we address one of the most fundamental questions about these modular functions $\mathrm{ch}_a(\tau)$: are they fixed by a congruence subgroup? The main results of this paper are Theorems 2 and 4. Other interesting results are the group presentations in Lemma 1, the explanations in §3, and the two propositions.

Let Γ denote $\mathrm{SL}_2(\mathbb{Z})$. By a *congruence subgroup* we mean any subgroup of Γ containing

$$\Gamma(N) := \{M \in \Gamma \mid M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}$$

for some N. $\Gamma(N)$ is called the principal congruence subgroup of level N. We are interested in whether a given representation ρ of Γ 'factors through a congruence subgroup', i.e. whether ρ sends $\Gamma(N)$ to the identity matrix I. This would tell us that ρ is actually a representation of the finite group

$$\mathrm{SL}_2(N) := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \Gamma/\Gamma(N)\ ,$$

consisting of all 2×2 matrices M with entries from the integers mod N and with determinant $|M| \equiv 1 \pmod{N}$. In other words, the matrices S and T would generate a group $\langle S, T\rangle$ isomorphic to some factor group of $\mathrm{SL}_2(N)$. We will say a given RCFT *has the* $\Gamma(N)$ *congruence property* if its modular representation ρ is trivial on some $\Gamma(N)$. This implies that its characters ch_a are all fixed by, i.e. modular for, $\Gamma(N)$. This would mean that the ch_a are all level N modular functions.

[1] Note that our choice of S is slightly different from that made by some other authors. This is discussed more fully four paragraphs into section 2.

See [AS,J] and references therein for some samples from the theory of noncongruence subgroups. The main reason congruence subgroups are so familiar is that they arise wherever theta functions of quadratic forms (or lattices) do, as was first shown by Hecke and Schoeneberg (*c.* 1940) — see for instance Chapter VI of [O] for details (our methods result in a new proof, given in section 4 below). In actual fact, *congruence subgroups are far rarer than noncongruence ones*: if we look at an arbitrary subgroup $\mathcal{G}$ of Γ with finite but large index $\|\Gamma/\mathcal{G}\|$, the probability will be almost 1 that it is noncongruence. More precisely [J], the number of noncongruence subgroups $\mathcal{G}$ of index $n = \|\Gamma/\mathcal{G}\|$ grows faster than $(\frac{n}{e})^{\frac{n}{6}}$, while the number of congruence subgroups of index n is bounded above by the much smaller number $n^{1+9\log_2 n}$.

Or for another indication of their comparative numbers, recall that given a subgroup $\mathcal{G}$ of Γ with finite index, we can construct the Riemann surface (with finitely many punctures) $\mathcal{G}\backslash\mathbb{H}$ from the upper half-plane $\mathbb{H}$. By the *genus* of $\mathcal{G}$ we mean the genus of that Riemann surface. Then for any given genus, there are only finitely many congruence subgroups $\mathcal{G}$ but infinitely many noncongruence subgroups [J].

$\mathrm{SL}_2(\mathbb{Z})$ is truly exceptional. By comparison, all finite-index subgroups of $\mathrm{SL}_n(\mathbb{Z})$, for $n \geq 3$, are congruence!

The first example of a noncongruence subgroup goes back to Klein (1879), and we can obtain infinitely many examples as follows. Consider the function $\xi(\tau) := \eta(\tau)/\eta(13\tau)$, where η is the Dedekind eta. Then ξ is a genus-zero modular function for $\Gamma(26)$, but for any $m = 2, 3, 4, \ldots$, its mth root $\xi(\tau)^{\frac{1}{m}}$ (taking the principal branch of $\log \xi$) is a genus-zero modular function for a *noncongruence* subgroup [AS].

Nevertheless, several people (e.g. [Mo,E,ES,DM,BCIR,B]) have conjectured (or at least speculated on the possibility of) the following:

CONJECTURE 1. *All RCFTs have the congruence property, so in particular their characters* $ch_a(\tau)$ *are modular functions for some* $\Gamma(N)$.

We will strengthen Conjecture 1 slightly, in §3.

Why is this conjecture not simply naive optimism? After all, it was not even known (see below) whether the subgroup of Γ fixing the ch_a has finite index. A reason for suspecting the truth of the conjecture is that all known RCFTs possess the congruence property — see for instance §4. But the best motivation for Conjecture 1 is the following hope, originally observed empirically by Atkin and Swinnerton-Dyer [AS]:

CONJECTURE 2. *Let* $f(\tau) = q^c \sum_{n=0}^{\infty} a_n\, q^{n/b} \not\equiv 0$ *be a modular function for some subgroup* $\mathcal{G}$ *of* Γ *and some* $b \in \mathbb{N}$, $c \in \mathbb{Q}$. *If the Fourier coefficients* a_n *are all algebraic integers, then* $\mathcal{G}$ *is a congruence subgroup.*

The most important examples of algebraic integers here are the 'rational integers' $\mathbb{Z}$, and the 'cyclotomic integers' $\mathbb{Z}[\xi_n]$ given by polynomials with coefficients in $\mathbb{Z}$, evaluated at some nth root of unity ξ_n.

The converse of Conjecture 2 is known to be true (see for example Ch. 6 of [L]): the modular functions for $\Gamma(N)$ with Fourier coefficients $a_k \in \mathbb{Z}[\xi_N]$ span the space of all modular functions for $\Gamma(N)$.

Now, the coefficients of our RCFT characters ch_a are in fact rational integers, so Conjecture 2 would imply Conjecture 1, at least if the RCFT characters were linearly

independent (which in general they aren't — we will return to this important point in §2). Thus Conjecture 2 strongly suggests (but in general won't imply) Conjecture 1. Although Conjecture 2 seems plausible and would be an important result in automorphic function theory, it remains unproven.

Why should we care about Conjecture 1? For one thing, congruence subgroups are much more familiar, and are also much better understood — relatively little is known generally about *non*congruence subgroups. The main technical difficulty with the latter is the lack for them of a satisfactory theory of Hecke operators. Whenever the rich theory of modular functions is applied to RCFT theory, a simplifying (and for many purposes necessary) assumption is certainly that the characters be modular for a congruence subgroup. See e.g. [ES] for such results, and [E] anticipates that the classification of all (not necessarily unitary) RCFTs with effective central charge $\tilde{c} \leq 1$, would follow quickly from some technical modular function results (Serre-Stark) and the congruence property. It would also be very useful to know that ρ is in fact a representation of the finite group $\mathrm{SL}_2(N)$, as those groups are so well-understood. For instance, their representations have been classified [TNW], and [E] suggested we should use that to classify the possible modular data in RCFTs obeying the congruence property.

By comparison, any finite group generated by an order 2 and an order 3 element together — e.g. the alternating group $\mathfrak{A}_n$ for $n \geq 9$ — will be a factor group of Γ (this is because $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the free product $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$). So we can't expect many interesting general results on the finite quotients $\Gamma/\mathcal{G}$, unless we assume in addition that e.g. $\mathcal{G}$ is a congruence subgroup.

In that sense, the main value of our paper could be to unlock a door behind which could lie some mathematical riches for RCFT.

Also, Conjecture 1 would help explain some curiousities in RCFTs (see §3 below). An example is the observation made in [BI] that the commutant for $A_\ell^{(1)}$ level k has an integral basis. More important is the Galois action for any RCFT [CG]: in §3 we will interpret this as the natural Galois action on level N modular functions [L].

To help put Conjecture 1 into perspective, consider the much weaker statement that the matrices S, T for any RCFT must necessarily generate a finite group (i.e. that the subgroup of Γ fixing all the characters $\mathrm{ch}_a(\tau)$ has finite index in Γ). Even that was not known to be true (but see Theorem 4 below). It is tempting to suspect that the obvious relations between S, T stated below in the second paragraph of §2 are enough to guarantee this. However, that is a false hope: in actual fact, the group defined by the presentation[2]

$$\langle S, T \,|\, T^N = S^4 = (ST)^3 = I, S^2 \text{ and } T \text{ commute}\rangle$$

equals $\mathrm{SL}_2(N)$ for $N \leq 5$ but is infinite for all $N > 5$. Imposing the additional condition $S^2 = I$ doesn't help: $\langle S, T\rangle$ then equals [CM] the symmetric group $\mathfrak{S}_3$ for $N = 2$, the tetrahedral group $\mathfrak{A}_4$ for $N = 3$, the octahedral group $\mathfrak{S}_4$ for $N = 4$, the icosahedral group $\mathfrak{A}_5$ for $N = 5$, and again is infinite for any $N > 5$. This $\langle S, T\rangle$ (with $S^2 = I$) is called the triangle (or polyhedral) group $(2, 3, N)$.

[2] To the left of the bar are the generators, to the right are the relations.

Thus for $\langle S,T\rangle$ to be finite, we need additional 'nonobvious' relations between the matrices S and T. (Imposing additional relations is equivalent to quotienting $(2,3,N)$ by some normal subgroup.) At least for N not a multiple of 6, we find in Theorem 2 exactly one additional relation that will accomplish this; moreover, it is easy to check this relation in practice and surprisingly when it holds (which we believe is always) it tells us this finite group will be a factor group of $\mathrm{SL}_2(N)$. Indeed, in Theorem 4 we apply this test to prove Conjecture 1 for N odd.

Incidentally, all finite factor groups of the triangle group $(2,3,6)$ have been classified by Newman (1964). The finite factor groups of (2,3,7) are important in Riemann surface theory and are called Hurwitz groups.

In the next section we give a simple test for determining whether or not a given RCFT has the congruence property, and we prove the congruence property when N is odd. While our test falls just short of establishing that all RCFTs (i.e. also N even) must have the congruence property, it demonstrates why generic RCFTs should. In the process we obtain natural presentations of the group $\mathrm{SL}_2(N)$. This simplifies the congruence subgroup test of [H], as we discuss briefly in §4.

2. When an RCFT has the congruence property

2.1. RCFT modular data. Consider the matrices S,T corresponding to a given RCFT. We will explicitly state in the next two paragraphs all properties of S,T we will need.

Because S and T correspond to a representation of Γ, we know $(ST)^3=I$, and the *charge-conjugation* matrix $C:=S^2$ commutes with both S and T. The matrices S,T are both unitary and symmetric, and T is diagonal. Also, we know [AM] there exists some integer $N>0$ for which $T^N=I$. Automatically in RCFT the characters are holomorphic in the upper half-plane. Incidentally, this also implies from (2) that each ch_a will be 'meromorphic at each cusp' — e.g. meromorphicity at the cusp $\mathrm{i}\infty$ would mean that each ch_a has a Laurent expansion in the local coordinate $q^{\frac{1}{N}}$. Hence the $\Gamma(N)$ congruence property would imply the characters are all level N modular functions (the converse is not necessarily true, because the characters will be linearly dependent in general — see below).

We know from [CG] that the entries S_{ab} of S must lie in a cyclotomic extension $\mathbb{Q}[\xi_n]$ of $\mathbb{Q}$. ξ_n here is the nth root of unity $\exp[2\pi\mathrm{i}/n]$, and $\mathbb{Q}[\xi_n]$ can be thought of as all complex numbers of the form $a_0+a_1\xi_n+\cdots+a_k\xi_n^k$, where the coefficients a_i are rational. The Galois group $\mathrm{Gal}(\mathbb{Q}[\xi_n]/\mathbb{Q})$ of $\mathbb{Q}[\xi_n]$ is defined to be the automorphisms of the field $\mathbb{Q}[\xi_n]$ which fix $\mathbb{Q}$. This Galois group is isomorphic to the multiplicative (mod n) group of integers coprime to n, which we write $\mathbb{Z}_n^*$: specifically, the Galois automorphism σ_ℓ corresponding to $\ell\in\mathbb{Z}_n^*$ takes the number $a_0+a_1\xi_n+\cdots+a_k\xi_n^k$ to $a_0+a_1\xi_n^\ell+\cdots+a_k\xi_n^{\ell k}$. Think of σ_ℓ as a generalisation of complex conjugation — in fact complex conjugation equals σ_{-1}. Now, choose any $\sigma\in\mathbb{Z}_n^*$, then [CG]

$$\sigma(S_{ab})=\epsilon_\sigma(a)\,S_{\sigma a,b}=\epsilon_\sigma(b)\,S_{a,\sigma b} \tag{3a}$$

where $\epsilon_\sigma(a)\in\{\pm1\}$ are signs, and $a\mapsto\sigma a$ defines a permutation of Φ, independent of b. If we define for each such σ the matrix G_σ given by $(G_\sigma)_{ab}=\epsilon_\sigma(a)\,\delta_{b,\sigma(a)}$, then the assignment $\sigma\mapsto G_\sigma$ defines a representation of $\mathbb{Z}_n^*$ and (3a) reads

$$\sigma(S)=G_\sigma S=SG_\sigma^{-1}\ . \tag{3b}$$

For instance, charge-conjugation $C = G_{-1}$. This important Galois action (3a) holds for any RCFT, and is a consequence of the basic properties of S, T given in the previous paragraph, together with the fact that the fusion coefficients N_{ab}^c in (1) are rational. All of these are basic ingredients in any RCFT [MS].

A minor clarification should be made. There is an equally valid alternate choice for S, namely $\rho \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, which is more commonly made in the literature, resulting in slightly different formulas. These two possibilities for S are complex conjugates of each other. For example our equations $(ST)^3 = (TS)^3 = I$ would become $(ST)^3 = (TS)^3 = C$. The choice we have made seems to result in slightly cleaner formulas.

Strictly speaking, the RCFT characters $\mathrm{ch}_a(\tau)$ will not in general be linearly independent and so equation (2a) will not uniquely determine S. The simplest example of this (there are others) is that a and its charge-conjugate Ca will always have equal characters $\mathrm{ch}_a = \mathrm{ch}_{Ca}$, even though often $a \neq Ca$. The obvious way out is to introduce additional variables in addition to τ, so ch_a then would involve a more 'sensitive' trace. The most familiar instance is the transition from the theta function $\theta(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2}$ to its Jacobi form $\theta(\tau, z) = \sum_{n\in\mathbb{Z}} q^{n^2/2} r^n$, where $q = e^{2\pi \mathrm{i}\tau}$ and $r = e^{2\pi \mathrm{i} z}$. This is precisely what is done for the affine Kac-Moody algebras [KP]. This technical point unfortunately is usually overlooked in the literature, and we will return to it in §3 (see also [GG]). Until it gets clarified though, and we learn how to obtain S unambiguously from the RCFT characters, it will be much more difficult to apply modular (or Jacobi) function theory rigourously and nontrivially to RCFT.

2.2. A natural presentation of $SL_2(N)$. A key tool we need are generators and relations for the finite group $\mathrm{SL}_2(N)$. There has been quite an industry in this direction (see e.g. [M,BM,CR,H,H2]). With a little effort we can write them in the following more transparent form.

LEMMA 1. *Choose any $N \in \{1, 2, 3, \ldots\}$. By '$\frac{1}{p}$' we mean the integer-valued multiplicative inverse of p mod N. Then we get the following presentations for $SL_2(N)$:*

(a) For N coprime to p, where p either equals 2 or 3,

$$\mathrm{SL}_2(N) = \langle s, t \,|\, t^N = s^4 = 1, (st^{-1})^3 = s^2,\ gs = sg^{-1},\ gt = t^{p^2} g \text{ where } g := st^{\frac{1}{p}} st^p st^{\frac{1}{p}} \rangle$$

(b) For N coprime to p, where p either equals 5 or 7,

$$\mathrm{SL}_2(N) = \langle s, t \,|\, t^N = s^4 = 1, (st^{-1})^3 = s^2, gs = sg^{-1}, gt = t^{p^2} g, g = t^{p\frac{p-1}{2}} st^{-\frac{2}{p}} st^{-\frac{p-1}{2}} st^2 s, \text{ where } g := st^{\frac{1}{p}} st^p st^{\frac{1}{p}} \rangle$$

(c) Write $N = 2^e m$ where m is odd. Let d be any integer satisfying the congruences $d \equiv 1$ (mod 2^e), $d \equiv 0$ (mod m). Write d_2 and d_3 for the multiplicative inverses (mod N) of $2 - d$ and $2d + 1$. Then

$$\mathrm{SL}_2(N) = \langle s, t \,|\, t^N = s^4 = [t^{2^e}, st^m s^{-1}] = [g_*, t] = 1,\ (st^{-1})^3 = s^2,\ g_* s = s g_*^{-1}, g_2 s = s g_2^{-1}, g_2 t = t^{4-3d} g_2, g_3 s = s g_3^{-1}, g_3 t = t^{8d+1} g_3, \text{ where } g_* := (st^{1-2d})^3, g_2 := st^{d_2} st^{2-d} st^{d_2}, g_3 := st^{d_3} st^{2d+1} st^{d_3} \rangle$$

Of course d in part (c) is guaranteed to exist, by the Chinese Remainder Theorem. By e.g. '$[g_*, t] = 1$' we mean that g_* and t commute. We have in mind here that $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $g = \begin{pmatrix} p & 0 \\ 0 & \frac{1}{p} \end{pmatrix} \longleftrightarrow G_p$. The monomial $st^m s^{-1}$ in (c) will then be $\begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}$. Note in (c) that $d_2 = \frac{1}{2}(1 + d + iN)$ where $d \equiv 1 + iN \pmod{2^{e+1}}$, and that $d_3 = 1 - \frac{2}{3}(d - jN)$ where $d \equiv jN \pmod{3^{f+1}}$ and 3^f is the power of 3 exactly dividing N. Since in all these cases $\mathrm{SL}_2(N)$ clearly satisfies the given relations, all we must prove here is that we have included enough relations. We won't use (b) in what follows. Our proof of the third presentation exploits the fact that $\mathrm{SL}_2(LM) \cong \mathrm{SL}_2(L) \times \mathrm{SL}_2(M)$ whenever L and M are coprime — we could have also used powers of 3 rather than 2. An important feature of our presentations is that the g's correspond to certain automorphisms of the group $\mathrm{SL}_2(N)$, as we will discuss in §3 and exploit shortly.

Proof of the Lemma. Writing $c := s^2$, we get in all three cases that c commutes with s and st^{-1}, hence with everything, and also that $(st)^3 = (ts)^3 = 1$.

To get a presentation for $\mathrm{SL}_2(N)$ when N is coprime to some prime p, it is enough to adjoin the relation '$t^N = 1$' to any presentation for the infinite group $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ where $\mathbb{Z}[\frac{1}{p}]$ denotes the ring $\{\frac{\ell}{p^i} \mid \ell, i \in \mathbb{Z}\}$. This important fact is a quick corollary of a deep theorem by Mennicke [M] showing that any finite subgroup of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ contains a congruence subgroup; the short proof of that corollary is given on p.1433 of [BM]. Presentations for $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ are given in [M] and most effectively [H2]. In particular, for $p = 2$ or 3 the presentation given in Theorem 5 of [H2] implies that whenever N is coprime with p, $\mathrm{SL}_2(N)$ is generated by x, y satisfying

$$xy^{-p}x = y^{-p}xy^{-p} \tag{4a}$$

$$(xy^{-p}x)^2 = (x^p y^{-1} x^p)^2 \tag{4b}$$

$$x^p y^{-1} x^p = y^{-1} x^p y^{-1} \tag{4c}$$

$$(xy^{-p}x)^4 = x^N = 1 \tag{4d}$$

Put $x = t$ and $y = st^{-\frac{1}{p}}s^{-1}$. It is enough to show, using the relations given in part (a), that this substitution satisfies the five relations in (4).

Now, $xy^{-p}x = tsts^{-1}t = s$ and $x^p y^{-1} x^p = t^p st^{\frac{1}{p}} s^{-1} t^p = t^p g t^{-\frac{1}{p}} s = gs$, so equations (4) say $s = sts^{-1}tsts^{-1}$, $s^2 = gsgs$, $gs = st^{\frac{1}{p}}s^{-1}t^p st^{\frac{1}{p}}s^{-1}$ and $s^4 = t^N = 1$, all of which clearly follow from the relations in part (a).

The proof of (b) is similar, and uses the presentation of $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ given on p.944 of [H2].

Finally, turn to the most difficult case: part (c). Define $S_e = t^d st^d st^d c$, $T_e = t^d$, $S_o = sS_e^{-1}$ and $T_o = t^{1-d}$, where $c = s^2$. We first want to show S_e and T_e commute with both S_o and T_o.

Begin with the observation that the relation $[t^{2^e}, st^m s^{-1}] = 1$ means, taking appropriate powers, that t^{d-1} and $st^d s^{-1} = st^d sc$ commute. Hence $st^d st^d st^d = t^{d-1}st^d stst^d =$

$t^{d-1}st^dt^{-1}sct^{-1}t^d = t^{d-1}st^{d-1}st^{d-1}c$, and by similar reasoning $t^dst^dst^ds = t^dstst^dst^{d-1} = t^{d-1}st^{d-1}st^{d-1}c$. Thus s and S_e commute, so so do S_e and S_o. This calculation says $S_o = (st^d)^{-3} = (t^ds)^{-3} = t^{1-d}st^{1-d}st^{1-d}c$, hence $T_e(st^d)^3 = (t^ds)^3T_e$ and so we get that S_o and T_e also commute.

By the same reasoning, $S_eT_o = t^dst^dstc = tst^dst^dc = T_oS_e$, so S_e and T_o commute. Trivially, T_e and T_o commute. Thus the subgroups $\mathcal{G}_e := \langle S_e, T_e\rangle$ and $\mathcal{G}_o := \langle S_o, T_o\rangle$ commute, and $\mathcal{G}_e \times \mathcal{G}_o$ equals the full group generated by s, t. We will be done if we can show $\mathcal{G}_e$ and $\mathcal{G}_o$ obey the $\mathrm{SL}_2(2^e)$ and $\mathrm{SL}_2(m)$ relations, obtained from (a).

Note that $g_*^2 = g_*(st^{1-2d})^3 = st^{1-2d}g_*^{-1}(st^{1-2d})^2st^{1-2d}t^{2d-1}s^{-1} = st^{1-2d}t^{2d-1}s^{-1} = 1$, so g_* has order 2 and commutes with both s, t. Define now $\alpha(s) = g_*s$ and $\alpha(t) = t^{1-2d}$. Because $\alpha(s)$ and $\alpha(t)$ obey all our relations in (c), α extends to a well-defined group endomorphism of $\langle s,t\rangle$ — in fact a group automorphism since $\alpha^2 = id$. (of course $(1-2d)^2 \equiv 1 \pmod N$)). Now, hit $t^{1-d}st^{1-d}st^{1-d}c = S_o = (st^d)^{-3}$ with α: we get $S_o = (g_*st^{-d})^{-3} = (t^ds)^3g_*c = S_o^{-1}g_*c$. Thus $S_o^2 = g_*c$, and hence $S_o^4 = 1$. Together with $s^4 = 1$, we get $S_e^4 = 1$. Now, $(S_eT_e)^3 = (S_o^{-1}sT_e)^3 = S_o^{-3}(st^d)^3 = S_o^{-4} = 1$ and hence also $(S_oT_o)^3 = 1$.

Finally, g_2 and g_3 obey the relations for g appearing in the $\mathrm{SL}_2(m)$ and $\mathrm{SL}_2(2^e)$ presentations obtained from (a); that we have both $g_2 \in \mathcal{G}_o$ and $g_3 \in \mathcal{G}_e$, can be seen by using two more automorphism arguments. Namely, define $\alpha_2(s) = g_2s$, $\alpha_2(t) = t^{2-d}$, then α_2 is seen to define an automorphism for our group $\langle s,t\rangle$. Evaluating $\alpha(1) = \alpha_2(S_oT_o)^3$ gives $1 = S_og_2^{-1}T_o^2g_2S_oT_o^2S_og_2^{-1}T_o = S_oT_o^{\frac{1}{2}}S_oT^2S_oT^{\frac{1}{2}}g_2^{-1}$, hence $g_2 = S_oT_o^{\frac{1}{2}}S_oT_o^2S_oT_o^{\frac{1}{2}}$ as it should. The proof for g_3 is identical. ■

The best presentation for $N = m$ odd is [CR]:

$$\mathrm{SL}_2(m) = \langle x, y \,|\, x^2 = (xy)^3,\ (xy^4xy^{(m+1)/2})^2y^mx^{2k} = 1\rangle$$

where $k := [m/3]$ (rounded down). This is optimal, in the sense that at least 2 generators are needed (since $\mathrm{SL}_2(m)$ isn't cyclic) and at least as many relations as generators are needed (since $\mathrm{SL}_2(m)$ is finite). More generally, for any finite group G, the number of relations minus the number of generators in any presentation must at least equal the rank of the 'Schur multiplier' $M(G)$ of G. $M(G)$ is always a finite abelian group; for $G = \mathrm{SL}_2(N)$ it was computed in [B1] and equals $\mathbb{Z}/2\mathbb{Z}$ whenever 4 divides N, otherwise it's trivial. Hence when 4 divides N, the best possible is 3 relations, but it seems 5 (the number we use) is the best that has been achieved thus far in the literature. Of course it goes without saying that the usefulness of a presentation is not merely determined by the number of generators and relations.

2.3. The congruence property for general RCFT. The following theorem is one of two main results in this paper.

THEOREM 2. *Consider any RCFT. Choose any integer N so that $T^N = I$. Then our RCFT has the $\Gamma(N)$ congruence property, provided either:*

(a) for N coprime to either $p = 2$ or $p = 3$, $G_pT = T^{p^2}G_p$;

(b) for arbitrary $N = 2^em$ where m is odd (let d be as in the Lemma), the following four relations all hold:

(i) T^{2^e} *commutes with* ST^mS^{-1}*;*
(ii) $G_{2d-1}\,T = T\,G_{2d-1}$*;*
(iii) $G_{2-d}\,T = T^{4-3d}\,G_{2-d}$*; and*
(iv) $G_{1+2d}\,T = T^{1+8d}\,G_{1+2d}$*.*

Proof. Consider first N in (a). Consider the equation $(ST)^3 = I$, and apply the Galois automorphism σ_p to it. We get $SG_p^{-1}T^pG_pST^pSG_p^{-1}T^p = I$, which we can simplify using (a) to get $S\,T^{\frac{1}{p}}\,S\,T^p\,S\,T^{\frac{1}{p}} = G_p$.

We find then that the assignments $s \mapsto S$, $t \mapsto T$, $g \mapsto G_p$ obey all the relations in the Lemma, proving Theorem 2(a).

The proof of Theorem 2(b) is similar. ■

In part (b), the matrix ST^mS^{-1} corresponds to the 2×2 matrix $\begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}$. We see that G_{1-2d} lies in the centre.

The conditions (a) and (b)(ii),(iii),(iv) appearing in Theorem 2 are surprisingly simple, and we show in Theorem 4 and §4 how easy they are to verify in practice. In (i), the roles of m and 2^e can be interchanged if it is more convenient. Also, we could just as easily use the factorisation $N = 3^f\ell$ for $\gcd(\ell,3) = 1$ and $\mathrm{SL}_2(N) \cong \mathrm{SL}_2(3^f) \times \mathrm{SL}_2(\ell)$, and make the appropriate changes to (i)–(iv).

Consider (i): it is equivalent to the statement

$$\mathcal{U}_{ac} := \sum_b S_{ab}S^*_{cb}T^m_{bb} = 0 \text{ unless } T^{2^e}_{aa} = T^{2^e}_{cc}\ . \tag{5}$$

This matrix $\mathcal{U}$ is symmetric and unitary, and has order 2^e. Note that for any $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}[S,T]/\mathbb{Q})$, $\sigma_\ell\mathcal{U}_{ac} = \epsilon_\ell(a)\,\epsilon_\ell(c)\,(\mathcal{U}^\ell)_{\sigma a,\sigma c}$. To see how (5) can be proved in practice, see section 4. We will have more to say about $\mathcal{U}$ shortly.

The converse of Theorem 2 can also be expected to hold: we expect (6a) below to hold for all ℓ, and condition (i) is a consequence of the factorisation $\mathrm{SL}_2(N) \cong \mathrm{SL}_2(m)\times\mathrm{SL}_2(2^e)$. In fact, if the characters ch_a were all linearly independent, then by the Galois action argument of §3, Theorem 2 would be an 'if and only if'.

2.4. Galois and T. Suppose now we have an RCFT which may or may not have the congruence property. In practice (see §4) it is easy to verify any condition of the form

$$G_\ell T = T^{\ell^2} G_\ell \tag{6a}$$

or equivalently

$$T_{\sigma_\ell a,\sigma_\ell a} = T^{\ell^2}_{aa}\ . \tag{6b}$$

Let us derive some easy consequences of (6a). Clearly, if ℓ obeys (6a), so does any $\pm\ell^j$.

Let M be an integer such that the cyclotomic field $\mathbb{Q}[\xi_M]$ contains all entries of S and T — we know it exists by [CG]. Then for any $\ell \in \mathbb{Z}^*_M$ obeying (6a), hitting $(ST)^3 = I$ with σ_ℓ gives

$$G_\ell = S\,T^{\frac{1}{\ell}}\,S\,T^\ell\,S\,T^{\frac{1}{\ell}} = T^\ell\,S\,T^{\frac{1}{\ell}}S\,T^\ell\,S\ . \tag{6c}$$

(6c) has two immediate consequences. Firstly, if $\ell\in\mathbb{Z}_M^*$ obeys (6c), then the group $\langle S,T\rangle$ has the automorphism defined by $S\mapsto G_\ell S$, $T\mapsto T^\ell$. The reason is that any relation between S and T (i.e. monomial $S^aT^b\cdots S^yT^z=I$) will also be obeyed by $\sigma_\ell(S)=G_\ell S$ and $\sigma_\ell T=T^\ell$ ((6c) is needed to tell us that $\sigma_\ell(S)\in\langle S,T\rangle$). Secondly, if the RCFT has the $\Gamma(M)$ congruence property and $\ell\in\mathbb{Z}_M^*$, then G_ℓ corresponds via ρ to the matrix $\begin{pmatrix}\ell & 0\\ 0 & \frac{1}{\ell}\end{pmatrix}\in\mathrm{SL}_2(M)$.

The following consequences of (6) are valid whether or not the congruence property holds.

Proposition 3. *Suppose (6b) is valid for all $\ell\in\mathbb{Z}_M^*$. Let N be the order of T: $T^N=I$.*

(a) Then $S_{ab}\in\mathbb{Q}(\xi_N)$ (i.e. we may take $M=N$ above).

(b) Suppose that all 'quantum-dimensions' $\frac{S_{a0}}{S_{00}}$ are rational. Then the central charge c is an integer.

(c) Fix any $b\in\Phi$. Choose any positive integer K_b for which all ratios $\frac{S_{ab}}{S_{0b}}$, as 'a' varies over Φ, lie in the cyclotomic field $\mathbb{Q}[\xi_{K_b}]$. Let M_b be least common multiple of K_b with the order of the root of unity T_{bb}. Then the ratio M_b/K_b is a divisor of 24 which is coprime to K_b.

Proof. If $\sigma_\ell T=T$, then $T^\ell=T$ so by (6c) we get $G_\ell=I$, i.e. $\sigma_\ell S=S$, and (a) holds.

Fix any $b\in\Phi$, and define $\mathbb{K}_b$ to be the field generated over $\mathbb{Q}$ by all ratios $\frac{S_{ab}}{S_{0b}}$ $\forall a\in\Phi$. So $\mathbb{K}_b\subseteq\mathbb{Q}[\xi_{K_b}]$. Of course $\frac{S^*_{ab}}{S_{0b}}=\frac{S_{Ca,b}}{S_{0b}}\in\mathbb{K}_b$ and $\frac{1}{S^2_{0b}}=\sum_a\frac{S_{ab}\,S^*_{ab}}{S^2_{0b}}\in\mathbb{K}_b$. Choose any $\sigma=\sigma_\ell\in\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{K}_b)$ — for instance any $\ell\equiv 1\pmod{K_b}$ will work. Then $S^2_{0b}=\sigma(S_{0b})^2=S^2_{0,\sigma b}$, so $S_{0b}=s\,S_{0,\sigma b}$ for some sign $s\in\{\pm1\}$. Hence $\frac{S_{ab}}{S_{0b}}=\sigma\frac{S_{ab}}{S_{0b}}=\frac{S_{a,\sigma b}}{S_{0,\sigma b}}=s\,\frac{S_{a,\sigma b}}{S_{0b}}$, i.e. $S_{ab}=s\,S_{a,\sigma b}$ $\forall a$. Unitarity of S forces $b=\sigma b$ (and $s=+1$). Now (6b) gives $T_{bb}^{\ell^2}=T_{bb}$.

In (b) we restrict to $b=0$, and we find that $T_{00}^{\ell^2}=T_{00}$ for all $\ell\in\mathbb{Z}_N^*$. But $T_{00}=\exp[-2\pi\mathrm{i}\,c/24]$. Let n be the denominator of the rational number $c/24$. Then $\ell^2\equiv1$ (mod n). But the 'definition of 24' says that that congruence can be satisfied for all $\ell\in\mathbb{Z}_n^*$, iff n divides 24. Hence $c\in\mathbb{Z}$.

The more general (c) is only slightly more complicated. Consider ℓ coprime to N, of the form $\ell=1+K_b\ell'$ for some ℓ'. We must have $\ell^2\equiv1$ (mod N_b), where N_b is the order of the root of unity T_{bb}. This means M_b/K_b must divide $(2+\ell')\ell'$. We are free to choose any ℓ' for which $1+K_b\ell'$ is coprime to N; the reader can quickly use that freedom to prove (c). ■

The 'definition of 24' is an easy-to-prove little fact about the number 24, which explains why that number appears in so many places. It states that for any $\ell\in\mathbb{Z}$, the relation $\ell^2\equiv1$ (mod n) holds for all ℓ coprime to n, iff n divides 24.

Examples of 3(b) are provided e.g. by the finite group orbifolds of holomorphic theories (see [DVVV], or §4.3 below), or by the WZW theories associated to e.g. $D_\ell^{(1)}$ level 2 when the rank ℓ is a perfect square.

Equations (6) also have consequences for (5). If (6a) holds for some ℓ, then we get

the alternate expression $\sigma_\ell \mathcal{U}_{ac} = (\mathcal{U}^{\frac{1}{\ell}})_{ac}$. Now, suppose (6a) holds for all Galois automorphisms σ_ℓ with $\ell \equiv 1 \pmod{2^e}$. Then $\sigma_\ell \mathcal{U}_{ac} = \mathcal{U}_{ac}$ for these ℓ, and hence $\mathcal{U}_{ac} \in \mathbb{Q}[\xi_{2^e}]$.

Let $\mathfrak{C}$ denote the *commutant* of the RCFT, i.e. the set of all complex matrices commuting with both S and T. This vector space is interesting because it contains the coefficient matrix of the genus-one partition function of the theory. Now, [BI] discovered the curious fact that the commutant of the affine algebra $A_\ell^{(1)}$ level k has a basis $M_1, \ldots, M_n$ consisting of integral matrices. This was later extended to all affine algebras. We will show in the next section that this is in fact a generic feature of RCFTs. For any Galois automorphism σ, applying σ to $M_a = SM_aS^*$ gives that M_a commutes with G_σ, and hence any $M \in \mathfrak{C}$ commutes with all G_σ. By the double-commutant theorem, we know then that each G_σ can be written as a polynomial in S, T. Equation (6c) finds that polynomial explicitly for us, provided (6a) holds for that σ.

The argument giving (6c) is quite general. In particular, consider now any RCFT — (6a) and the congruence property may or may not be satisfied. Write $T_{(\ell)} := G_\ell T^{\frac{1}{\ell^2}} G_\ell^{-1}$; it is diagonal, with entries $T_{(\ell)aa} = T^{\frac{1}{\ell^2}}_{\sigma_\ell a, \sigma_\ell a}$. Equations (6) hold iff $T_{(\ell)} = T$. The argument giving (6c) now yields

$$G_\ell = ST^{\frac{1}{\ell}} ST^{\ell}_{(\ell)} ST^{\frac{1}{\ell}} = T^\ell S T^{\frac{1}{\ell}}_{(\frac{1}{\ell})} ST^\ell S = ST^{\frac{1}{\ell}}_{(\frac{1}{\ell})} ST^\ell ST^{\frac{1}{\ell}}_{(\frac{1}{\ell})} = T^\ell_{(\ell)} ST^{\frac{1}{\ell}} ST^\ell_{(\ell)} S \tag{7}$$

Again, (7) holds in complete generality. Since by construction the matrix G_ℓ is real, we also get $G_\ell = ST^{*\frac{1}{\ell}} ST^{*\ell}_{(\ell)} ST^{*\frac{1}{\ell}} C$ etc. We are now ready for our second main result.

2.5. The congruence property for RCFTs when T has odd order.

THEOREM 4. *Consider any RCFT. Let N be the order of T: i.e. $T^N = I$. If N is odd, then the RCFT obeys the $\Gamma(N)$ congruence property.*

Proof. It was shown in [By] that for any $a, b \in \Phi$, the number

$$\mathcal{Z}(a,b) := T_{00}^{\frac{1}{2}} T_{bb}^{*\frac{1}{2}} \sum_{x,y \in \Phi} N_{xy}^a S_{bx} S_{0y} T_{yy}^2 T_{xx}^{-2} \tag{8}$$

is an integer, among other things. We can interpret all fractions as integers (mod N), as usual. Consider the matrix $\mathcal{Z}^{(a)} := T^{\frac{1}{2}} ST^2 N_a T^{*2} ST^{*\frac{1}{2}}$ where N_a is the fusion matrix $(N_a)_{bc} = N_{ab}^c$. Write $T_h := T_{(\frac{1}{2})}$; we know from (7) that $G_2 = ST_h^{*\frac{1}{2}} ST^{*2} ST_h^{*\frac{1}{2}} C$ and $G_{\frac{1}{2}} = T_h^{\frac{1}{2}} ST^2 ST_h^{\frac{1}{2}} S$. Thus we can write

$$\begin{aligned}
\mathcal{Z}^{(a)} &= T^{\frac{1}{2}} T_h^{*\frac{1}{2}} (G_{\frac{1}{2}} ST_h^{*\frac{1}{2}} S) N_a (ST_h^{\frac{1}{2}} SG_2 C) T_h^{\frac{1}{2}} T^{*\frac{1}{2}} \\
&= T^{\frac{1}{2}} T_h^{*\frac{1}{2}} G_{\frac{1}{2}} ST_h^{*\frac{1}{2}} D_a T_h^{\frac{1}{2}} SG_2 T_h^{\frac{1}{2}} T^{*\frac{1}{2}}
\end{aligned}$$

where D_a is the diagonal matrix with entries $(D_a)_{xx} = \frac{S_{ax}}{S_{0x}}$ (we used the Verlinde formula (1) here). Since D_a and T_h are both diagonal, they commute and we get

$$\mathcal{Z}^{(a)} = T^{\frac{1}{2}} T_h^{*\frac{1}{2}} G_{\frac{1}{2}} N_{Ca} G_2 T_h^{\frac{1}{2}} T^{*\frac{1}{2}} \ .$$

Put $\alpha = T_{00}T^*_{h\,00}$, then (8) tells us

$$\sqrt{\alpha}\,\epsilon_{\frac{1}{2}}(0)\,\epsilon_{\frac{1}{2}}(b)\,N_{Ca,\sigma_{\frac{1}{2}}0}^{\sigma_{\frac{1}{2}}b}\,T^{\frac{1}{2}}_{h\,bb}\,T^{*\frac{1}{2}}_{bb} \in \mathbb{Z}$$

for all $a, b \in \Phi$. Hence $\alpha\, T_{h\,bb}\, T^*_{bb} \in \mathbb{Q}$ for all b. But it is also an Nth root of unity, and N is odd, so we find $T = \alpha T_h = \alpha T_{(\frac{1}{2})}$. Therefore

$$\begin{aligned} I = G_2 G_{\frac{1}{2}} &= (\alpha^{-1} S T^{\frac{1}{2}} S T^2 S T^{\frac{1}{2}})(\alpha^{-1} T^{\frac{1}{2}} S T^2 S T^{\frac{1}{2}} S) \\ &= \alpha^{-2} S T^{\frac{1}{2}} S T^2 (T^{-1} S T^{-1} C) T^2 S T^{\frac{1}{2}} S = \alpha^{-2} S T^{\frac{1}{2}} (T^{-1}) T^{\frac{1}{2}} S C = \alpha^{-2} I \end{aligned}$$

where we made repeated use of $(ST)^3 = I$. Hence $\alpha = 1$ and $T = T_{(\frac{1}{2})}$, and by Theorem 2(a) we are done. ■

For clarity, let us repeat the properties of RCFTs used in deriving Theorems 2 and 4. We used the facts that S and T are both unitary and symmetric, and that T is diagonal and of finite order. We used Verlinde's formula (1), or at least the fact that that formula always yields rational numbers (it should in fact give nonnegative integers). Finally, the derivation of (8) in [By] required elementary properties of the $(N^b_{aa} \times N^b_{aa})$ braiding matrix $\mathcal{R}^{[b]}_{aa}$ ($= \Omega^b_{aa}$ in the notation of [MS]): he needs its square and trace. All of these are standard properties of RCFTs [MS].

The condition that T has odd order, can be rephrased in terms of more elementary quantities of RCFT, namely the central charge c and the conformal weights h_i. First note that we can write any rational number r uniquely as a product of prime numbers raised to certain integral powers: $r = \prod p_i^{a_i}$. Let $t(r)$ denote the 'two-ness' of r, i.e. the exponent of 2 in this prime decomposition of r. For example, $t(2.4) = 2, t(\frac{5}{3}) = 0, t(33.5) = -1$. Then T has odd order, iff $t(c) \geq 3$ and $t(h_i) \geq 0$ for all i.

2.6. Further problems. Additional directions suggested by this work are the following. Roughly, they involve the interplay between three topics: the congruence property, equations (6), and the number fields $\mathbb{Q}[S]$ and $\mathbb{Q}[T]$. See also Conjecture 3 next section.

- Can we prove (6a) uniformly for all RCFT? Take any Galois automorphism σ_ℓ, and apply σ_ℓ^2 to the equation $(ST)^3 = I$. We get $(G_\ell S G_\ell^{-1} T^{\ell^2})^3 = I$, i.e.

$$(ST')^3 = I\ , \text{ where } T' := G_\ell^{-1} T^{\ell^2} G_\ell = T_{(\frac{1}{\ell})} \tag{9}$$

  We want to show $T' = T$. The point is that the equation $(ST)^3 = I$ is strong and almost uniquely determines T from S, given the facts that T is diagonal and of finite order. It could be useful to understand to what extent these conditions do determine T. Clearly, given one solution T of $(ST)^3 = I$, we can always obtain another by multiplying the matrix by a third root of unity. If S is real, then T^* will be another solution. For a given S there can be additional 'sporadic' solutions for T, but there doesn't seem to be that many. Thus (9) can be interpreted as suggesting that (6a) will generically hold.

- In the case (b) of Theorem 2 (i.e. N a multiple of 6), if we drop e.g. condition (i), can we at least show that the matrices S and T generate a *finite* group?
- When we have the congruence property, we should be able to prove equations (6) for all ℓ. An approach is discussed next section, but it requires additional knowledge of the RCFT characters.
- Conversely, it is tempting to believe that if equations (6) hold for all ℓ, then we should have the congruence property. Of course the only question is proving (5) when N is a multiple of 6. We could accomplish this if we knew that for any N, $\mathrm{SL}_2(N)$ has a presentation of the form

$$\mathrm{SL}_2(N) \cong \langle s, t \,|\, t^N = s^4 = 1, (st^{-1})^3 = s^2,\, g_a s = s g_a^{-1},\, g_a t = t^{a^2} g_a,\, g_a g_b = g_b g_a$$
$$\text{where } g_a := s t^{\frac{1}{a}} s t^a s t^{\frac{1}{a}} \text{ for all } a, b \in \mathbb{Z}_N^* \rangle$$

  Lemma 1 says that this convenient but terribly inefficient presentation works whenever N is not a multiple of 6. We expect this presentation to hold for all N, but we don't know a proof. Can anyone help us?
- To our knowledge, the powers of the matrix $STS^{-1} = \rho(\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix})$ have been largely ignored in RCFT and the studies of the associated representations of the modular group, but they do play a role in the mathematical theory, as Theorem 2(b) demonstrates. We give an example of how to study this, at the beginning of section 4.
- We expect that the $\Gamma(N)$ congruence property should imply that all entries S_{ab} lie in the cyclotomic field $\mathbb{Q}[\xi_N]$. We know [CG] the S_{ab} lie in *some* cyclotomic field, but the question here is whether they lie in that specific one. We know this will hold if (6) holds for all ℓ. We know from basic results in modular functions theory (see e.g. [L]) that the Fourier coefficients for each $\mathrm{ch}_a(-1/\tau)$ will lie in $\mathbb{Q}[\xi_N]$ provided ch_a is fixed by $\Gamma(N)$. This last statement is sometimes (see e.g. [ES]) taken (prematurely it seems to us) to imply that each $S_{ab} \in \mathbb{Q}[\xi_N]$ when the $\Gamma(N)$ congruence property holds. The problem is the usual one: the characters $\mathrm{ch}_a(\tau)$ in an RCFT won't in general be linearly independent, so we can't read off S from (2a). We will return to this question next section.
- The automorphism group of each $\mathrm{PSL}_2(p^n)$ is known [MD], and from this it is straightforward to obtain the automorphism group of each $\mathrm{SL}_2(p^n)$. In particular, for $p > 5$ the automorphisms are generated by the Galois ones $s \mapsto g_\ell s$, $t \mapsto t^\ell$ for each ℓ coprime to p, together with the inner ones $a \mapsto bab^{-1}$ for each $b \in \mathrm{SL}_2(p^n)$ — in particular the outer automorphism group $\mathrm{Out}(\mathrm{SL}_2(p^n)) \cong \mathbb{Z}/2\mathbb{Z}$. There are additional automorphisms for $p = 2, 3, 5$. Perhaps it can be hoped that for some N, there will be some kind of generalisation of the Galois action (3) corresponding to nonGalois automorphisms in $\mathrm{Out}(\mathrm{SL}_2(N))$. We briefly return to this next section.
- It is clearly desirable to try to extend our results to any rational vertex operator algebra. The main barrier is that Verlinde's formula (1) is not yet known to give rationals there (or even to be defined!). Theorem 1 in [DLM] shows that for any rational VOA obeying the technical finiteness condition 'C_2', T will have finite order. Again subject to the C_2 condition, Theorem 5.3.3 in [Z] (see also Theorem 3 in [DLM]) shows

that the characters $\mathrm{ch}_a(\tau)$ for a rational VOA will all be holomorphic in the upper half-plane, and define a representation of $\mathrm{SL}_2(\mathbb{Z})$. This C_2 condition is conjectured to hold for all rational VOAs. A discussion of VOAs in RCFT is provided e.g. by [H3].

3. Explaining some curiousities

See also [B] for some related comments.

3.1. The RCFT Galois action reinterpreted. The Galois action [CG] in RCFT seems somewhat mysterious, but actually it is a special case of one known since early this century. A cyclotomic Galois action arises naturally in modular functions (see e.g. Chapter 6 of [L]). In particular, let $f(\tau)=q^c\,\sum_{n=0}^\infty a_nq^{n/N}$ be a modular function for $\Gamma(N)$, with coefficients a_n in $\mathbb{Q}[\xi_N]$. Choose any $\ell\in\mathbb{Z}_N^*$ and write h_ℓ for any matrix in Γ congruent (mod N) to $\begin{pmatrix}\ell & 0\\ 0 & \frac{1}{\ell}\end{pmatrix}$. Then we get the remarkable formula [L]

$$f(h_\ell\tau)=q^c\,\sum_{n=0}^\infty \sigma_\ell(a_n)\,q^{n/N} \tag{10a}$$

which will also be a modular function for $\Gamma(N)$.

Now let $\mathrm{ch}_a(\tau)$ be the characters for an RCFT obeying the congruence property. Apply this Galois action to $\mathrm{ch}_a(s\tau)$: we find

$$\mathrm{ch}_a(h_\ell s\tau)=\sum_{b\in\Phi}\sigma_\ell(S_{ab})\,\mathrm{ch}_b(\tau) \tag{10b}$$

and hence $\rho(h_\ell)=G_\ell$, as in (6c).

As mentioned in §2, arguments of these kind break down in most RCFTs, because they assume that the RCFT characters are linearly independent. Introducing additional variables into VOA (hence RCFT) characters can be done quite generally, as will be discussed more fully in [GG]. Variants of Jacobi forms [EZ] often arise in this way (these have a 'linear' $\vec{z}$-dependence as well as the 'quadratic' τ dependence, in analogy with the function theta $\theta(\tau,z)$ discussed in §2). Jacobi forms behave essentially the same as modular functions, and the analogue of the cyclotomic Galois action was worked out in [Be] (he restricted to a single variable z, but his argument extends to vectors $\vec{z}$). We find that the above $\rho(h_\ell)=G_\ell$ observation carries over. Also, the representation of Γ (or $\mathrm{SL}_2(N)$) arising from these Jacobi functions will have matrix entries in the field $\mathbb{Q}[\xi_N]$.

$\mathrm{SL}_2(N)$ has automorphisms defined by $s\mapsto h_\ell s$, $t\mapsto t^\ell$, for any $\ell\in\mathbb{Z}_N^*$. Looking at t, it is easy to show that the ℓth automorphism is *inner* (i.e. given by $M\mapsto VMV^{-1}$ for some $V\in\mathrm{SL}_2(N)$), iff ℓ is a perfect square mod N. These automorphisms are precisely the Galois actions on modular functions for congruent subgroups, and are precisely the Galois actions in RCFT when that RCFT obeys the congruence property. Thus in hindsight it seems that we should have taken the presence of the RCFT Galois action of [CG] as a strong hint that the Γ representation ρ there factors through a congruence subgroup, or, if we already suspected that ρ factors through one, then we should have started looking for an action on our RCFT data of the Galois group $\mathbb{Z}_N^*$.

This discussion, and the results of our paper, lead us to propose the following strengthening of Conjecture 1:

CONJECTURE 3. *All RCFTs have the* $\Gamma(N)$ *congruence property, where* N *is the order of* T*: in particular* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mapsto S$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto T$ *defines a representation of* $SL_2(N)$*. In addition, each entry* S_{ab} *lies in* $\mathbb{Q}[\xi_N]$*, where* $\xi_N := \exp[2\pi \mathrm{i}/N]$*, and equations (6) hold for all* $\sigma \in \mathrm{Gal}(\mathbb{Q}[\xi_N]/\mathbb{Q})$*.*

3.2. Integral bases for commutants. The congruence property can also be used to provide an explanation for the existence of an integral basis for the commutant (see the discussion near the end of §2.4). In particular:

PROPOSITION 5. *Suppose the matrices* S *and* T *obey both the* $\Gamma(N)$ *congruence property as well as equations (6). Let* $\mathfrak{C}$ *denote all the complex matrices* M *commuting with both* S *and* T*. Then* $\mathfrak{C}$ *has a basis (over* $\mathbb{C}$*) consisting of integral matrices.*

Proof. We know from Proposition 3 that the entries of S, T lie in the cyclotomic field $\mathbb{Q}[\xi_N]$. Certainly $\mathfrak{C}$ will have a basis $M_1, \ldots, M_n$ with entries from $\mathbb{Q}[\xi_N]$. Rescaling M_1 appropriately, we may assume some entry $(M_1)_{i_1,j_1}$ equals 1. Subtracting M_1 from the other M_a, we can assume all other $(M_a)_{i_1,j_1} = 0$. Continue inductively in this way: we get indices $(i_1, j_1), \ldots, (i_n, j_n)$ such that $(M_a)_{i_b,j_b} = \delta_{ab}$.

Choose any $M \in \mathfrak{C}$ with entries from $\mathbb{Q}[\xi_N]$, and any Galois automorphism $\sigma = \sigma_\ell$. Then M commutes with the matrix G_σ, by (6c). From the calculations

$$\begin{aligned} S(\sigma M)S^{-1} &= \sigma((SG_\sigma)\, M(G_\sigma^{-1}S^{-1})) = \sigma M \ , \\ T(\sigma_\ell M)T^{-1} &= \sigma_\ell(T^{\frac{1}{\ell}} M T^{-\frac{1}{\ell}}) = \sigma_\ell M \ , \end{aligned}$$

we see that σM also lies in $\mathfrak{C}$.

Now let $\overline{M}_a = \sum \sigma M_a$, where the sum is over all $\sigma \in \mathrm{Gal}(\mathbb{Q}[\xi_N]/\mathbb{Q})$. Then $\overline{M}_a$ will have rational entries, they will be linearly independent, and they will all lie in $\mathfrak{C}$. Hence they constitute a basis for $\mathfrak{C}$. ■

3.3. The observations of Bantay. We will conclude with a discussion of the remarkable observation in [By]: the numbers $\mathcal{Z}(a,b)$ defined in (8) are integers, congruent to N_{aa}^b (mod 2), and $|\mathcal{Z}(a,b)| \le N_{aa}^b$. This observation seems highly nontrivial: for instance taking $a = 0$ tells us that

$$\sqrt{T_{00}T_{bb}^*} \sum_d S_{db}S_{0d} = \pm\delta_{0b}$$

where the sum is over all self-conjugate d (i.e. all $d = Cd$), and this seems difficult to prove without using either the methods of [By] or this paper.

That the $\mathcal{Z}(a,b)$ are integers played an important role in our proof of Theorem 4. Assuming T has odd order, we can turn the Theorem 4 argument around now, and what we find is $\mathcal{Z}^{(a)} = G_{\frac{1}{2}} N_{Ca} G_2$, where the matrix $\mathcal{Z}^{(a)}$ is defined in the proof of Theorem 4. $\mathcal{Z}(a,b)$ is the $(0, Cb)$ entry of $\mathcal{Z}^{(Ca)}$, namely

$$\mathcal{Z}(a,b) = \epsilon_{\frac{1}{2}}(0)\, \epsilon_{\frac{1}{2}}(b)\, N_{a,\sigma 0}^{C\sigma b}$$

where for readability we write σ for the Galois permutation $\sigma_{\frac{1}{2}}$. So $\mathcal{Z}(a,b)$ will indeed always be an integer, at least when N is odd. This is a consequence of the fact that the N odd RCFT must obey the congruence property (i.e. Theorem 4). The remainder of Bantay's observation now reduces to

$$N_{a,\sigma 0}^{\sigma b} \equiv N_{aa}^{Cb} \pmod 2 \qquad \text{and} \qquad N_{a,\sigma 0}^{\sigma b} \leq N_{aa}^{Cb}$$

which cannot be proved using the methods of this paper. Nevertheless, we see that Bantay's 'Frobenius-Schur indicator' $\mathcal{Z}(a,0)$, which equals 0 or ± 1 if $Ca \neq a$ or a is real/pseudo-real, respectively, will never be negative here. Hence:

COROLLARY 6. *When T has odd order, the RCFT will have no pseudo-real primary fields.*

In addition, for N odd we get the surprising fact that there exists an $a \in \Phi$ (namely $a = \sigma_{\frac{1}{2}} 0$) with the property that $N_{aa}^{b} \neq 0$ iff $b = Cb$, in which case $N_{aa}^{b} = 1$. In a colourful phrase suggested to us by M.A. Walton,

the sum of the self-conjugate primary fields has a (fusion) square-root!

For a concrete example, the affine algebra $A_2^{(1)}$ at even level k has N odd, and $\sigma_{\frac{1}{2}} 0$ there equals the weight $(0, \frac{k}{2}, \frac{k}{2})$. Hence we get the fusion rules

$$(0, \frac{k}{2}, \frac{k}{2}) \times (0, \frac{k}{2}, \frac{k}{2}) = (k,0,0), (k-2,1,1), \ldots, (0, \frac{k}{2}, \frac{k}{2}) \ ,$$

with all multiplicities equal to 1.

Note that in fact we have shown a little more: *any* entry of $\mathcal{Z}^{(a)}$ is manifestly an integer. Thus this aspect of [By] can be generalised, at least for odd N: the quantities

$$\mathcal{Z}(a,b,d) := \sqrt{T_{dd} T_{bb}^{*}} \sum_{x,y \in \Phi} N_{xy}^{a} S_{bx} S_{dy} T_{yy}^{2} T_{xx}^{*2} = \epsilon_{\frac{1}{2}}(d)\, \epsilon_{\frac{1}{2}}(b)\, N_{a,\sigma d}^{C\sigma b}$$

will always be integers, for any $a, b, d \in \Phi$ (the case $d = 0$ reduces to [By]). Also, there is nothing special about the number '2' here. In particular, let ℓ be coprime to the order N of T (which we no longer assume to be odd), and assume that ℓ satisfies (6a). Then the numbers

$$\mathcal{Z}_{\ell}(a,b,d) := T_{dd}^{\frac{1}{\ell}} T_{bb}^{*\frac{1}{\ell}} \sum_{x,y \in \Phi} N_{xy}^{a} S_{bx} S_{dy} T_{yy}^{\ell} T_{xx}^{*\ell}$$

will all be integral. It would be very interesting to find an interpretation for those numbers.

4. Examples

4.1. Lattice theories. Consider first the RCFT corresponding to a single compactified boson, or equivalently a 1-dimensional lattice theory or U(1) theory. Take the lattice to be $\sqrt{n}\mathbb{Z}$ where n is an even integer. The primary fields are labelled by $a \in \{0, 1, \ldots, n-1\} = \Phi$. The (full-variable) character for $a \in \Phi$ is proportional to $\Psi_a(n\tau, \sqrt{n}z) = \sum_{m \in \mathbb{Z}} \exp[2\pi \mathrm{i} \sqrt{n}\, (m + \frac{a}{n}) z + n\pi \mathrm{i}\, (m + \frac{a}{n})^2 \tau]$. The transformation law of the Ψ_a can be

read off from that of $\theta_3(\tau,z)=\Psi_0(\tau,z)$, first found by Poisson and Jacobi (*c.* 1830). The resulting S and T matrices are

$$S_{ab}=\frac{1}{\sqrt{n}}\exp[2\pi\mathrm{i}\frac{ab}{n}]\ ,\qquad T_{ab}=\exp[\pi\mathrm{i}\frac{a^2}{n}-\pi\mathrm{i}\frac{1}{12}]\,\delta_{ab}\ .$$

We already know this theory satisfies the congruence property, because the characters are theta functions. However let's try to see it from Theorem 2. The order N here is the least-common-multiple of 24 and $2n$. The Galois permutation is $\sigma_\ell a=\ell a$ taken mod n, for any ℓ coprime to n. Equation (6b) then is obviously satisfied, so it suffices to verify (5). Now, $\mathcal{U}_{ac}=\frac{\exp[-\pi\mathrm{i}m/12]}{n}S(m,2a-2c,n)$, where $S(a,b,c)$ is the *generalised Gauss sum*

$$S(a,b,c):=\sum_{k=0}^{c-1}\exp[\pi\mathrm{i}\,(ak^2+bk)/c]\ .$$

$S(a,b,c)$ obeys an important symmetry, called *reciprocity*, due originally to Genocchi (1852) — see e.g. [Bt] for a modern proof and generalisation. In particular,

$$S(a,b,c)=\sqrt{\left|\frac{c}{a}\right|}\exp[\pi\mathrm{i}\,\{\mathrm{sgn}(ac)-b^2/ac\}/4]\,S(-c,-b,a)\ .$$

Applying this to $\mathcal{U}_{ac}$, we find

$$\mathcal{U}_{ac}=\frac{\exp[\pi\mathrm{i}\,(-m/12+1/4-(a-c)^2/mn)]}{\sqrt{mn}}\sum_{b=0}^{m-1}e^{2\pi\mathrm{i}\,(c-a)b/m}$$

using the facts that m divides n, and m is odd and n even. Hence $\mathcal{U}_{ac}\neq 0$ iff m divides $a-c$, which implies that m divides a^2-c^2, and we are done.

Note that this gives an immediate proof that for any n-dimensional even Euclidean lattice Λ, and any vector $g\in\Lambda^*$ (the dual lattice), the Jacobi theta function

$$\Theta(g+\Lambda)(\tau,z):=\sum_{x\in g+\Lambda}\exp[\pi\mathrm{i}x^2\tau+2\pi\mathrm{i}x\cdot z]$$

will be fixed by some $\Gamma(N)$ (up to the usual factors). Indeed, we can express $\Theta(g+\Lambda)$ as a homogeneous degree n polynomial in the 1-dimensional Ψ_a by using Gram-Schmidt to find in Λ an n-dimensional orthogonal sublattice.

4.2. Affine theories. Consider next any affine algebra $X_r^{(1)}$ at level k. There is associated a well-known representation S,T of Γ [KP] — the primaries are labelled by the highest-weights $\lambda\in P_+^k(X_r)$, and for instance we have

$$T_{\lambda\lambda}=\exp[\pi\mathrm{i}\,\frac{(\lambda+\rho)^2}{k+h^\vee}-\pi\mathrm{i}\,\frac{\dim X_r}{12}]\ .$$

Because of the (Jacobi) theta function expression for the affine characters, we again know this representation of Γ factors through $\Gamma(N)$, where N can be taken to be $(k+h^\vee)n$ for some n (e.g. $n=24\,(r+1)$ works for $A_r^{(1)}$). Provided N is not a multiple of 6 (e.g. $A_r^{(1)}$ level k when k and r are both even) this also follows from Theorem 2, as we'll now see.

Equations (6) are trivial to verify for the affine algebras: for any Galois automorphism, $\sigma_\ell(\lambda)$ can be interpreted as the unique weight $\lambda^+ \in P_+^k(X_r)$ for which

$$\lambda^+ + \rho = w(\ell(\lambda+\rho)) + (k+h^\vee)\alpha$$

where w lies in the (finite) Weyl group and α lies in the coroot lattice of X_r. Hence the norms $\ell^2(\lambda+\rho)^2$ and $(\lambda^+ +\rho)^2$ are congruent mod $2(k+h^\vee)$, so relation (6b) holds — the constant factor $\exp[-\pi\mathrm{i}\dim X_r/12]$ in $T_{\lambda\lambda}$ causes no problems, because of the 'definition of 24':

$$\gcd(\ell,24)=1 \;\Rightarrow\; \ell^2\equiv 1 \pmod{24}\ .$$

4.3. Orbifold theories. Another important, and in many ways behaviourally opposite, example of RCFT modular data, is associated to any finite (discrete) group G [DVVV]. For any $a\in G$, the conjugacy class associated to a is the set of all elements of the form $g^{-1}ag$. Fix a set R consisting of one representative for each conjugacy class of G. By $C_G(a)$ we mean the centraliser of a in G: i.e. the subgroup consisting of all elements in G which commute with a. The primary fields here are pairs (a,χ), where $a\in R$ and χ is the character of an irreducible representation of $C_G(a)$. Here

$$T_{(a,\chi),(b,\chi')} = \delta_{a,b}\,\delta_{\chi,\chi'}\,\frac{\chi(a)}{\chi(e)}$$

where e is the identity of G. This data corresponds to the RCFT obtained by orbifolding a holomorphic RCFT by G.

The order N of T here is the exponent of G (i.e. the smallest positive integer such that $a^N=e$ for all $a\in G$). Again, it was already known that the corresponding modular data factors through $\Gamma(N)$. One way to see this follows from the treatment in [KSSB]. Let $\mathcal{C}(G)$ be the space of all functions $f: G\times G\to\mathbb{C}$ satisfying two conditions: $f(g,h)=0$ unless $gh=hg$, and $f(aga^{-1},aha^{-1})=f(g,h)\ \forall a\in G$. Γ acts on these by $f((g,h)\begin{pmatrix}a&b\\c&d\end{pmatrix})=f(g^ah^c,g^bh^d)$. (This strange-looking action of Γ on $G\times G$ is related to the natural action of Γ on the fundamental group $\pi_1(\text{torus})\cong\mathbb{Z}^2$.) This turns out to be the Γ representation appearing in the RCFT — this construction shows that its kernel clearly contains $\Gamma(N)$.

Once again, it is immediate that (6b) holds. In particular, the Galois permutation (3) takes (a,χ) to $(ba^\ell b^{-1},\sigma_\ell\chi^{b^{-1}})$, where $b\in G$ is chosen so that $ba^\ell b^{-1}\in R$, and χ^g denotes the function $\chi^g(h):=\chi(ghg^{-1})$. Thus $T_{\sigma(a,\chi),\sigma(a,\chi)}=\sigma^2 T_{(a,\chi),(a,\chi)}$, which is (6b).

4.4. The congruence test of Hsu. Finally, we should point out that Lemma 1 provides a presentation for $\mathrm{SL}_2(N)$ which may be more natural and hence useful than the one given in [H] for N even but not a power of 2. In this case, Hsu [H] combined the generators and relations of Mennicke and Behr [M,BM] to obtain the following presentation of $\mathrm{SL}_2(N)$.

Write $N = 2^e m$ where m is odd, and define d as in Lemma 1. Then a presentation for $\mathrm{SL}_2(N)$ is

$$\langle L, R \,|\, L^N = [a,r] = [b,l] = (ab^{-1}a)^4 = (lr^{-1}l)^4 = 1, (ab^{-1}a)^2 = (b^{-1}a)^3 = (b^2 a^{-\frac{1}{2}})^3,$$
$$(lr^{-1}l)^2 = (r^{-1}l)^3 = (sr^5 lr^{-1}l)^3, (lr^{-1}l)^{-1}s(lr^{-1}l) = s^{-1}, s^{-1}rs = r^{25},$$
$$\text{where } a = L^{1-d}, b = R^{1-d}, l = L^d, r = R^d, s = l^{20}r^{\frac{1}{5}}l^{-4}r^{-1}\rangle$$

The advantage of ours, perhaps, is that our relations involve the automorphisms of the group and so should be easier to identify and verify in practice. This may permit a practical simplification of the congruence subgroup test in [H]. We also have one fewer relation.

Fewer relations even than Lemma 1(c) would be obtained by using the 2 relation presentation of $\mathrm{SL}_2(\mathrm{odd})$ in [CR], together with e.g. our 5 relation presentation of $\mathrm{SL}_2(2^e)$. It should be pointed out that provided N is not a multiple of 210, a much better presentation of $\mathrm{SL}_2(N)$ (with at most 6 relations) is given by our Lemma 1(a),(b).

Acknowledgements. T.G. thanks C. Cummins, J. McKay, D. McNeilly, P. Moree and M. Walton for various conversations, and A.C. thanks D. Altschuler, M. Bauer, J. Lascoux, J. Wolfart, and J.-B. Zuber. We both thank W. Nahm and P. Ruelle. This paper was written in part while both authors were visiting IHES, whom we thank for their generous hospitality. The research of T.G. was supported in part by NSERC.

Bibliography

[AM] G. Anderson and G. Moore, "Rationality in conformal field theory", Commun. Math. Phys. **117** (1988), 441–450;
C. Vafa, "Towards classification of conformal field theories", Phys. Lett. **B206** (1988), 421–426.

[AS] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, "Modular forms on noncongruence subgroups", In: Proc. Symp. Pure Math. **19** (AMS, Providence, 1971), ed. by T. S. Motzkin, pp.1–26.

[By] P. Bantay, "The Frobenius-Schur indicator in conformal field theory", Phys. Lett. **B394** (1997), 87–88.

[B] M. Bauer, "Galois actions for genus one rational conformal field theories", In: *The Mathematical Beauty of Physics*, (World Scientific, 1997) pp. 152–186.

[BCIR] M. Bauer, A. Coste, C. Itzykson, and P. Ruelle, "Comments on the links between su(3) modular invariants, simple factors in the Jacobian of Fermat curves, and rational triangular billiards", J. Geom. Phys. **22** (1997), 134–189.

[BI] M. Bauer and C. Itzykson, "Modular transformations of SU(N) affine characters and their commutant", Commun. Math. Phys. **127** (1990), 617–636.

[BM] H. Behr and J. Mennicke, "A presentation of the groups PSL(2, p)", Can. J. Math. **20** (1968), 1432–1438.

[Bt] B.C. Berndt, "On Gaussian sums and other exponential sums with periodic coefficients", Duke Math. J. **40** (1973), 145–156.

[Be] R. Berndt, "Zur Arithmetik der elliptischen Funktionenkörper höherer Stufe", J. Reine Angew. Math. **326** (1981), 79–94.

[Bl] F. Beyl, "The Schur multiplicator of $\mathrm{SL}(2, Z/mZ)$ and the congruence subgroup property", Math. Z. **191** (1986), 23–42.

[CR] C. M. Campbell and E. F. Robertson, "A deficiency zero presentation of SL(2,p)", Bull. London Math. Soc. **12** (1980), 17–20.

[CG] A. Coste and T. Gannon, "Remarks on Galois symmetry in RCFT", Phys. Lett. **B323** (1994), 316–321.

[C] A. Coste, "Investigations sur les caractères de Kac Moody et quelques quotients de $\mathrm{SL}(2, Z)$", IHES preprint P/97/78, to e-appear, and refs therein.

[CM] H. M. S. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 4th edn. (Springer, Berlin, 1980).

[DVVV] R. Dijkgraaf, C. Vafa, E. Verlinde, and H. Verlinde, "The operator algebra of orbifold models", Commun. Math. Phys. **123** (1989), 485–526.

[DM] C. Dong and G. Mason, "Vertex operator algebras and Moonshine: a survey", In: Adv. Stud. Pure Math. **24** (Math. Soc. Japan, Tokyo, 1996), ed. by E. Bannai and A. Munemasa, pp.101–136.

[DLM] C. Dong, H. Li, and G. Mason, "Modular-invariance of trace functions in orbifold theory", preprint q-alg/9703016.

[E] W. Eholzer, "On the classification of modular fusion algebras", Commun. Math. Phys. **172** (1995), 623–660.

[ES] W. Eholzer and N.-P. Skoruppa, "Modular invariance and uniqueness of conformal characters", Commun. Math. Phys. **174** (1995), 117–136.

[EZ] M. Eichler and D. Zagier, *The Theory of Jacobi Forms*, (Birkhäuser, Boston, 1985).

[GG] M. Gaberdiel and T. Gannon, "The characters of rational conformal field theory and vertex operator algebras", work in progress.

[H] T. Hsu, "Identifying congruence subgroups of the modular group", Proc. Amer. Math. Soc. **124** (1996), 1351–1359.

[H3] Y.-Z. Huang, "Vertex operator algebras and conformal field theory", Int. J. Mod. Phys. **A7** (1992), 2109–2151.

[H2] J. Hurrelbrink, "On presentations of $\mathrm{SL}_n(\mathbb{Z}_S)$", Commun. Alg. **11** (1983), 937–947.

[J] G. A. Jones, "Congruence and non-congruence subgroups of the modular group: a survey", In: *Proceedings of Groups—St. Andrews 1985* (Cambridge University, Cambridge, 1986), pp.223–234.

[KP] V. G. Kac and D. Peterson, "Infinite–dimensional Lie algebras, theta functions and modular forms", Adv. Math. **53** (1984), 125–264.

[KSSB] T. H. Koornwinder, B. J. Schroers, J. K. Slinkerland, and F. A. Bais, "Fourier Transform and the Verlinde Formula for the quantum-double of a finite group", math.QA/9904029.

[L] S. Lang, *Elliptic Functions*, 2nd edn. (Springer, 1987).

[MD] D. L. McQuillan, "Some results on the linear fractional groups", Illinois J. Math. **10** (1966), 24–38;
J. B. Dennin, Jr., "The automorphisms and conjugacy classes of $LF(2,2^n)$", Illinois J. Math. **19** (1975), 542–552.

[M] J. Mennicke, "On Ihara's modular group", Invent. math. **4** (1967), 202–228.

[Mo] G. Moore, "Atkin-Lehner symmetry", Nucl. Phys. **B293** (1987), 139–188.

[MS] G. Moore and N. Seiberg, "Classical and quantum conformal field theory", Commun. Math. Phys. **123** (1989), 177–254.

[O] A. Ogg, *Modular forms and Dirichlet series*, (Benjamin, New York, 1969).

[TNW] S. Tanaka, "Irreducible representations of the binary modular congruence groups mod p^λ", J. Math. Kyoto Univ. **7** (1967), 123–132;
A. Nobs and J. Wolfart, "Die irreduziblen Darstellungen der Gruppen $SL_2(Z_p)$, insbesondere $SL_2(Z_2)$. I,II.", Comment. Math. Helvetici **51** (1976), 465–526.

[Z] Y. Zhu, "Modular invariance of characters of vertex operator algebras", J. Amer. Math. Soc. **9** (1996), 237–302.